Herding Cats:
Operationalize… man!

April 2011

BrandenWilliams
SECURE BUSINESS GROWTH

Security operations management isn't the most well defined or well executed thing that we do as security professionals. It's not quite as nebulous as our definition of cloud computing, but for the most part we don't have executable plans or a way to demonstrate value back to an organization on a daily basis. In fact, this either tends to get exposed or lauded when a security incident occurs. Part of the reason why, I believe, is because of how broad of a brush we use when describing operational management. Sure, it might include things like responding to security events, collecting and correlating logs, and other operational things you might do daily. But I've seen some definitions wide enough to include things that you might do to demonstrate compliance with a security standard, and some as granular as to suggest that a penetration test of a remote outpost might be included as well.

In my mind, security operations management should do at least these three things very well: demonstrate value from system event visibility into real-time, security related activity in the enterprise; cover all elements of high-value assets (i.e., manage both the physical and electronic worlds); and support the audit side of the business by providing defensible work product documenting the execution of security controls.

Just like other cyclical things in enterprise information technology, it appears that the operations management piece goes through the in-sourced versus out-sourced swing on a periodic basis. My customers are telling me that we are on the in-source swing. Many companies are pulling in key elements of operations management like incident response and event management away from outsourced partners with one exception, the cloud. For companies looking to reduce risk in their business for certain non-core activities, service providers are being asked to step up to more responsibility (and liability in many cases) and provide business solutions instead of tactical activities.

For example, one of my customers recently reviewed how they process and respond to security events and incidents, and invested in both people and hardware to bring the activity in house for their core business operations. In the same motion, one of their non-core businesses operations pushed more responsibility to their outsourced provider with respect to e-commerce to the point of simply getting wire transfers and pick lists from that organization. In their view, they were focusing their operational expenditure on high-value, core assets that the business must have running well for their global operations, and simply reducing a non-core revenue stream slightly to allow the service provider to provide added services required to meet my customer's security and IT service level agreements.

One of the big problems that large companies have is tracking risk against high-value assets outside of their corporate headquarters. Should a company look to expand its business into a previously untapped market, they must first evaluate the business risk of doing so and make sure the benefit to the company exceeds this (to the risk appetite of the board). But once they make the decision to jump into the market, they must continuously monitor and adjust the controls protecting their high-value assets[1]. Without a process (and tools to support) to handle information related to these assets, companies will often be limited to responding to events instead of anticipating or preventing them.

Finally, controls are great when they work, but if someone outside of your company (or even inside) wants to verify that the controls function, you will need to present defensible

FOOTNOTES

[1] These might fall into any of the following categories: people, intellectual property, manufacturing equipment, cash, or other expensive assets used in the value-producing area of that business.

evidence to support that notion. Any part of an IT or info-sec control must contain some way to create defensible evidence to show that the control works. Information security, when done in a vacuum, does not breed trust within the enterprise. When things look like a black box, they are trusted less than things based on open standards and architectures.

As IT transforms to a service-based model, we as security professionals must not only adapt, but also contribute value back to our organizations such that we support the longevity of the business. If you take a look at your company's ability to operationally manage security and it doesn't function today, what makes you think it will function in the new world of IT? Before you get too far down the road, it might be time to take a hard look at your organization's ability to operate security enterprise wide.

About the Author:

Branden R. Williams, CISSP, CISM, CPISA/M, has been making a name for himself in the Information Technology and Security arena since 1994, as a high school Junior. Now, a graduate of University of Texas, Arlington earning his BBA in 2000 with a concentration in Marketing and the University of Dallas, where he earned an MBA in Supply Chain Management & Market Logistics, in 2004, Williams is sought after as both an Adjunct Professor and Information Technology & Security Strategy Leader in the corporate world.

Williams regularly assists top global retailers, financial institutions, and multinationals with their information security initiatives. Read his blog, buy his book, or reach him directly at http://www.brandenwilliams.com/.

TEL 214 727 8227
FAX 214 432 6174
BLOG brandenwilliams.com
EMAIL brw@brandenwilliams.com

brandenwilliams
SECURE BUSINESS GROWTH